STATE OF ILLINOIS

ILLINOIS COMMERCE COMMISSION

Illinois Commerce Commission On Its Own Motion	:	
	:	16-NOI-01
Notice of Inquiry Regarding the Regulatory Treatment of Cloud-Based Solutions	:	

NOTICE OF INQUIRY

I. Background

Cloud computing generally refers to delivering computing power – whether in the form of software, storage capacity, or other services – over the Internet. Web-based software services, more commonly referred to as cloud computing or Software-as-a-Service ("SaaS"), are being implemented globally by users in virtually all types of organizations, including manufacturing, government, services, retail, and some utilities.

In September 2015, the Illinois Commerce Commission ("Commission") hosted a policy session on Business and IT Investments in Cloud Computing Arrangements ("Policy Session"). The purpose of the Policy Session was to discuss technology advancements in energy analytics and cloud computing arrangements, including the regulatory accounting treatment of such arrangements as capital expenses versus operating expenses. According to current accounting principles, utility investment in on-premises software is treated as a capital expense, which is included as part of the utility's rate base on which it is allowed a return. Contrastingly, utility investment in a cloud-based solution is treated as an operating expense, which does not earn a rate of return. A simple illustration of the distinction is that a utility is permitted to capitalize the cost of purchasing a copy of Microsoft's on-premises Office product but not the cost of a

license for Microsoft's cloud product known as Office 365, despite having similar functionality.

Cloud proponents and utility representatives at the Policy Session stressed that the traditional utility model incents investment in on-premises IT software solutions over cloud solutions without regard to technical or functional merits because utilities favor fixed assets that go into rate base. Moreover, they pointed to the benefits of bringing together the various IT systems within the utility to enable data sharing, data analysis, and interoperability. For example, utilities pursuing SaaS options can improve existing business functions, such as customer relationship management, while also exploring applications like Smart Meter as a Service. According to its proponents, a shift to the cloud can enable both utilities and customers to leverage the economic and environmental value of the smart grid by aggregating systems to analyze the relevant data, develop new products and programs to help customers reduce their energy bills, and help utilities to better manage the power infrastructure.

As innovation becomes increasingly necessary for grid modernization, the Commission is interested in determining whether utility investment in cloud computing is prudent and whether leveling the playing field between cloud and on-premises solutions would encourage utilities to make the most cost-effective investments. As described in detail in Section IV, below, the Commission is interested in: 1) comparing cloud services with on-premises IT systems, looking at respective cost, reliability, and security; 2) examining the regulatory accounting treatment of cloud services and discerning whether there are additional regulatory barriers that hinder the adoption of cloud services; and 3) exploring whether additional benefits would accrue from deployment of cloud-based

solutions to utilities, customers, the grid, and the environment.

Accordingly, the Commission initiates this Notice of Inquiry ("NOI") as a vehicle for gathering information and opinions that may form the basis for action by the Commission on these matters.

II. Applicable Law – NOI

The Commission's rules with respect to NOIs are found in 2 Ill. Adm. Code 1700, Subpart D. Section 1700.330 states that NOIs will contain, in part, a disclaimer that:

> the Notice of Inquiry proceeding is not a rulemaking, but that information gathered may or may not form the basis for the initiation of rulemaking or for other purposes at a later date.

2 Ill. Adm. Code § 1700.330.

III. NOI Manager

Section 1700.310 of the Commission's NOI rules requires the designation of an NOI Manager to conduct discussions as are necessary to address the issues raised in the Commission's directive for an NOI. The NOI Managers in this case will be Elizabeth McErlean and Anastasia Palivos. For correspondence, please note:

Mailing Address:

Elizabeth McErlean & Anastasia Palivos
Illinois Commerce Commission
160 North LaSalle, Ste. C- 800 Chicago, IL 60601

Telephone: 312-814-8929/4088
Fax: 312-814-1818
e-mail: emcerlean@icc.illinois.gov & apalivos@icc.illinois.gov

IV. NOI Questions and Issues

Interested persons and entities are requested to respond to the following questions and issues:

Cloud vs. On-Premises IT Solutions:

1. Identify how costs differ between a traditional on-premises IT system and a cloud-based solution, including all relevant costs and timing of costs.
2. Describe the costs associated with migrating utility data systems to cloud services. What evidence have stakeholders seen of this shift and what are the results? How long would it take to migrate utility data from on-premises IT to a cloud solution? Provide examples of utility services that have migrated from utility-owned systems to cloud services.
3. Identify costs associated with training employees to use cloud-based solutions and whether those costs differ substantially from costs to train employees to use utility-owned, on-premises systems.
4. Describe whether and how operations and maintenance costs differ between utility-owned, on-premises systems and cloud services.

B. Reliability:

1. Describe whether and how cloud-based solutions improve safety and reliability at a utility.

   Splunk offers a 100% SLA, Fedramp certified, GovCloud solution, including:

   - Secure: Completed SOC2 Type 2 Attestation* and ISO 27001certification*. Dedicated cloud environments for each customer.
   - Reliable: 100% Uptime SLA. 10TB+ scalability. All the features of Splunk Enterprise, including apps, APIs and SDKs.
   - Hybrid: Centralized visibility across Splunk Cloud (SaaS) and Splunk Enterprise (software) deployments.
   - Please also refer to: SPLUNK CLOUD.PDF

2. Proven Cloud Technologies in Regulated Utilities
   i. Identify the cloud services that have proven most successful for public utilities. Identify the differences between a public versus a private cloud, and determine whether one is more appropriate for the utility industry.
   ii. Identify public utilities that have adopted cloud-based solutions and what effect cloud services have had on the utility's safety and reliability.
   iii. Identify circumstances where the utility and its customers are better served by a combination of utility-owned, on-premises IT systems and cloud services, a "hybrid" model. What approach best maximizes reliability, safety and security for a utility and its customers?
3. Identify successful cloud services adopted by non-utility, but highly regulated, companies or industries. Explain any lessons from their

experience that can help maximize reliability, safety, and security for a utility and its customers.

C. Cybersecurity: -

1. Cloud Security

i. Describe whether and how utilities will benefit from the cybersecurity practices provided by cloud-based solutions providers versus those associated with on-premises solutions.

Utilities are faced with adapting to a dynamic threat landscape, evolving adversary tactics, advanced threats and changing business demands—and your existing security technologies can't keep up. To meet these new challenges, modern security teams need analytics capabilities and contextual incident response; and they must be able to rapidly implement new threat detection techniques to reduce time-to-threat response and make business-centric decisions. Security teams can more quickly detect, respond and disrupt attacks by centralizing and leveraging all machine data.

Splunk Enterprise Security in the Cloud is a premium security solution that enables security teams to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk, and safeguard your business. Splunk ES Cloud enables your security teams to use all data to gain organization-wide visibility and security intelligence. ES can be used for continuous monitoring, incident response, running a security operations center or for providing executives a window into business risk. Splunk ES Cloud enables SOC (Security Operations Centers) to focus on the identification, mitigation and remediation of security breaches while the core infrastructure that runs the solution is in a distributed, FEDRAMP certified, 100% SLA enforced operating environment. This configuration enables customer to focus on the core practice of security while infrastructure is managed wholly by Splunk.

ii. Identify any cybersecurity benefits of using a cloud-based solution versus an on-premises IT system.

- 100% SLA
- For a successful SOC, on prem customers must constantly enrich their data with threat intelligence such as IP blacklists, malware signatures, phish attack information, threat domain and other threat artifacts.
- Splunk Enterprise Security Cloud automates these updates for the customers as a managed service, thus enabling the most up to date threat intel as a managed service within the Splunk Cloud environment

2. New Risks
    i. Describe the extent of new risks introduced (if any) when a utility migrates to a cloud-based solution from an existing on-premises system.

When sending any data over the wire, exposure to risk is evident. However, Splunk Cloud uses industry standard SSL encryption for data in transit from Forwarders to the Splunk Indexers. Data can be forwarded over any TCP port and uses a proprietary transport protocol wrapped within SSL.

Further, all data transmission between Splunk instances (e.g. forwarder to indexer, indexer to client browser) can be strongly encrypted (SSLv2/3). All data transmission between third-party devices such as firewalls or intrusion detection systems (IDS) can be strongly encrypted as long as the third-party device supports strong ciphering and hashing and can perform a standard handshake with other devices. Additionally Splunk has software that provide reliable, secure data collection from remote sources\xFF and forward that data into Splunk called Universal Forwarders. The Splunk Universal Forwarder can be centrally managed and installed on the OS of the machine containing the data source to locally collect the data and then send it to Splunk indexer. The Universal Forwarder has the ability to send data to an indexer via TCP (more reliable than UDP), encrypted via SSL, and in a throttled manner so as to not overwhelm network connections. It can also cache data should the connection to the Splunk indexer be lost. Another benefit is that the Universal Forwarder can be configured to automatically load balance events across multiple Splunk indexers.

In addition, Splunk Cloud operates within Amazon Web Services (AWS). All AWS data centers have attained the certifications and attestations below:
• SOC 2 Type 2
• PCI Data Security Standard (PCI-DSS) Level 1
• ISO 27001
• Cloud Security Alliance
• DoD Information Assurance Certification and Accreditation Process (DIACAP)
• Federal Information Security Management Act (FISMA)

All data centers running Splunk Cloud are securely monitored 24x7.

Physical access of AWS facilities is strictly limited to select AWS staff only.

Splunk Cloud offers data encryption at rest using AES 256-bit encryption*. At present, Splunk Cloud customers have to work with Splunk Cloud Support to manage their encryption keys. Splunk Cloud's backup/archiving process encrypts customer data within separate Simple Storage Service (S3) buckets using AES 256-bit encryption. Keys are rotated on a routine basis and are under continuous monitoring. Archiving takes place when customer hot buckets roll to warm buckets, a process that regularly occurs based on every 10GB of data ingested or every 24 hours (whichever comes first).

Please refer to attachment: SAFEGUARDING CUSTOMER DATA IN SPLUNK CLOUD.PDF

3. Incident Response
    i. Describe how cloud-based solution providers can respond to cybersecurity threats in contrast to utilities utilizing on-premises systems.

Splunk Enterprise Security Cloud enables the view of a single event or a roll-up of related system events and an incident management workflow for security teams. Users can easily verify incidents, change their status and criticality, and transfer among team members, all while supplying mandatory comments about status changes. Status changes are audited, monitored and tracked for team metrics. If the State were to entertain a managed service, threat intel can be shared across per State entities for greater oversight in terms of the threat landscape and remediation activities, this is difficult to do in a single on premise environment.

4. Threat Detection
    i. Describe whether and how a cloud-based solution can assist a utility in protecting, detecting, and responding to cybersecurity threats and operational vulnerabilities.

Splunk Enterprise Security Cloud enables security teams to use all data to gain organization-wide visibility and security intelligence. Splunk ES Cloud can be used for continuous monitoring, incident response, running a security operations center or for providing executives a window into business risk.
Splunk ES Cloud provides organizations the ability to:

- Improve security operations with faster response times
- Improve security posture by getting end-to-end visibility across all machine data
- Increase detection capabilities using analytics-driven security
- Make better informed decisions by leveraging threat intelligence

Improve Security Posture

Security Posture

Get a library of security posture widgets to place on any dashboard or easily create your own. See security events by location, host, source type, asset groupings and geography. KPIs provide trending and monitoring of your security posture.

Incident Review and Classification

View a single event or get a roll-up of related system events and an incident management workflow for security teams. Easily verify incidents, change their status and criticality, and transfer among team members, all while supplying mandatory comments about status changes. Status changes are audited, monitored and tracked for team metrics.

Built on a Big Data Platform for Security Intelligence

Spunk ES leverages Splunk Enterprise capabilities that include:

- **Index Any Data Source.** The ability to bring in any data without custom connectors or vendor support enables analysts to quickly access, search and analyze the data they need to complete their investigation.
- **Scalability.** The ability to index hundreds of terabytes of data per day. Splunk does not apply a schema at the time data is indexed and searches across terabytes of data can be performed quickly.
- **Flexible Dashboards—**Dashboards can be easily created or customized for a quick graphical view of any data or correlation that is important to the organization. Organize multiple dashboards on a single screen for a customized view of the organization's overall security posture.
- **Ad Hoc Searches.** Ad hoc searches enable security teams to quickly understand what attacks are occurring in their environment to determine the best course of action.

Improve Security Operations

Customizable Dashboards

Create your own security portal based on your role and the things that matter to your organization. Organize and correlate multiple

data sources visually in a single user interface to find relationships and gain context.

Asset Investigator
Visually correlate events over time for any IP address. This helps the analyst gain insight into time relationships across events.

Unified Search Editor
Use a user-friendly, consistent search creation experience—including guided searches—for key security indicator or key performance indicator correlation searches, and identity and asset investigation visualizations.

Statistical Analysis
Pre-built dashboards will help you identify anomalies in event and protocol data. The dashboards are pre-built using auto-configuring thresholds and baselines.

Incident Review, Classification and Investigation
Splunk ES provides comprehensive incident review capabilities that include:

- Drill down from graphical elements to raw data and wire data captures to gain an understanding of all network communications
- Unique workflow actions that augment the security investigation process and allow you to pivot on a single piece of common information—or any other data—to rapidly develop the threat context
- Classification that allows for bulk event reassignment, changes in status and criticality classification, with all analyst activity available for auditing purposes

Incident Review Audit
For governance, auditing and protection against tampering, Splunk ES provides reports on all Splunk user and system activities for a complete audit trail. The Splunk platform uses data signing to maintain chain-of-custody and detect any alterations to the original log and event data.

Detect Internal and Advanced Threats

Asset Center/Identity Center
Understanding where assets are, who owns them, their criticality and who should be accessing information on systems helps prioritize security events and investigations. Splunk software has the ability to perform lookups of data stored in an

asset database, active directory, spreadsheet or CSV file and use that information as context for security events in reports and dashboards.

Advanced Threat Investigation
Use a variety of advanced detection and investigative controls for investigative purposes or to detect abnormal activity that's often associated with compromised systems. This includes DNS new domain analysis, HTTP category and user agent analysis, traffic size analysis, URL length analysis, and threat intelligence artifacts.

Visual Anomaly Detection
View event data in the form of swim lanes and use heat maps to quickly identify anomalous behaviors and trends related to assets and identities in the environment. Out-of-the-box swim lanes include authentications, endpoint changes, threat list activity, IDS attacks, malware attacks, notable events and risk modifiers related to the user. Swim lanes can be modified to provide user activity profiling across any network, endpoint, access, identity and threat intelligence source.

Protocol Intelligence
Get information from the wire that's either in lieu of, or complementary to, data from the endpoint or network, or could otherwise not be obtained. Provides protocol information supported by the Splunk App for Stream including SSL, DNS and email activity.

Identify, Prioritize and Manage Security Events

Splunk ES delivers a flexible yet powerful security framework that enables security teams to:

Manage Alerts
The Incident Review Framework facilitates incident tracking from the time a correlation rule first triggers an incident, or notable event, all the way through the closure of the investigation. Notable events can be annotated, assigned to an owner for investigation and further examined to gain context around the assets or identities involved, the specific rules that were triggered and the associated raw events.

Assign Risk

The Risk Scoring Framework enables a risk score to be applied to any event asset, behavior or user based on relative importance or value to the business. This helps security teams to prioritize alerts based on predefined thresholds, while also exposing contributing factors of the risk to all relevant teams. Easily track their security status to understand and actively manage overall business risk.

Operationalize Threat Intelligence

The Threat Intelligence Framework enables organizations to automatically collect, aggregate and de-duplicate threat feeds from a broad set of sources including open sources, subscription based, law enforcement, local and shared from other organizations. This includes integrated support for next-generation security standards such as STIX, TAXII and openIOC. Risk scores can be assigned to that threat intelligence and used to enhance incident investigation, breach investigation and scoping. Through a cloud based, managed service, these feads can be updated by such a third party enabling the State to focus on its core operations while having most up date security intel.

Quickly Identify Security Events

The Notable Event Framework helps identify notable events and track the actions analysts take to resolve the issues that triggered security events. It facilitates the task of triaging notable events, including search filters, tagging and sorting.

Understand Identity and Privilege Levels

The Identity and Asset Framework enables the automatic mapping of data stored in an asset database, active directory, spreadsheet or CSV file. This information can then be used as context for security events in reports and dashboards.

Access Protection

Simplify access control monitoring, exception analysis and audit processes for applications, operating systems and identity management systems across the enterprise. Satisfy compliance and forensics requirements to track highly privileged users and system access attempts on any business-critical application.

Endpoint Protection

Increase the effectiveness of endpoint security products such as Symantec™ Endpoint Protection, IBM® Proventia Desktop or McAfee® Endpoint Protection. Prioritize threats and view long term trends. Endpoint Protection includes searches, reports and a library of alerts for malware, rare activities, resource utilization and availability.

Network Protection
Monitor and detect events from network and security devices across the enterprise. Discover anomalies across firewalls, routers, DHCP, wireless access points, load balancers, intrusion detection sensors and data loss prevention devices. Capabilities include correlations, searches, reports and dashboards for monitoring, alerting and reporting on network-based events. Statistical analysis is employed on proxy data to understand HTTP-based behavioral outliers.

Make Better Informed Decisions

Enhance incident response and investigations by leveraging and correlating data from a broad set of sources, including security and non-security data collected from across the organization, and supplemented with internal and external threat intelligence and other contextual information.
Splunk ES leverages Splunk Enterprise to bring in any data without custom connectors or vendor support, enabling new data sources to be utilized quickly and easily, without expensive and time-consuming professional services engagements. In addition, Splunk ES natively supports emerging threat intelligence sharing standards such as STIX, TAXII and openIOC. Threat Intelligence feeds can be operationalized by aggregating multiple sources, formats and retrieval mechanism, de-duplicating the information and then alerting on them as well as extracting the values for use in investigations as well as for downstream actions.

Optimize Incident Response

Streamline investigations of dynamic, multi-step attacks and more easily see the relative time relationship between the various events to determine root cause and next steps. Facilitate collaboration across the organization by enabling any security team member to place events, actions and annotations onto a timeline to share their perspective of the scenario.

Investigator Journal
Similar to a web browser history, the Investigator Journal logs certain analyst activities taken throughout the investigation without the need for multiple tabs and separate tools. This enables analysts to focus on tracking attack activities while the system tracks the investigation, actions and notes. The Investigator Journal enables analysts to easily:

- Track searches and activities

- Review activities at any point
- Select and place into timeline for temporal analysis
- Help remember searches, steps taken, provide annotation support

Investigation Timeline

The Investigation Timeline enables analysts to investigate the sequence of events using the kill chain methodology to determine the attack lifecycle. At any point in the investigation they can add relevant actions from the Investigator Journal, as well as raw events and even their own notes, to a timeline. This enables them to visualize and more clearly understand the attack details, as well as the sequential relationship between various events – and quickly determine the appropriate next steps.

The timeline makes it easy to collaborate with team members and other security personnel throughout the organization. In addition to being able to click through the entire report to get the original analyst's perspective, any security team member can place events, actions and annotations into a timeline to share their perspective on the scenario.

The investigative reporting feature combines the raw event, actions, annotation notes and investigators involved with the incident so that team members can scroll through the details to understand the sequencing and time relationships of multiple events. This also helps executives and new analysts understand how attacks occurr in their environment and how to investigate them.

Please refer to: SPLUNK ENTERPRISE SECURITY.PDF

5. Security Framework for Utilities
    i. Identify the key elements and value of a security best-practices framework for utilities to address cybersecurity threats.

Splunk maps to the CIS CRITICAL SECURITY CONTROLS as a framework for security Best Practices. Splunk provides a single, integrated, security intelligence platform that allows today's security professionals to ensure that their organizations are meeting Critical Security Controls requirements. The software can verify incoming data, execute the requirements needed, or support human activities associated with a control. Security professionals find Splunk software uniquely suited to support these controls in a number of ways, including: universal data ingestion with no specific vendor preference; a real-time schema-less architecture; unparalleled

scaling capabilities for big data; and an agile and flexible reporting interface.

How Splunk Software Maps to the CIS CSC: Four Approaches Splunk software maps to each control in the CIS CSC (see Figure

There are four major ways in which the Splunk platform supports the controls:

Verification:
As Splunk software ingests data, it can generate reports and dashboards that show compliance or non-compliance with controls. Incidents of non-compliance can generate alerts to SOC personnel.

Execution:
In the case of an attack or non-compliance, Splunk software can carry out recommended actions to meet controls. With version 6.0 of the CIS CSC, Splunk software becomes even more critical, since control 14 surrounding audit logs has been promoted to position 6.

Verification & Execution
Data from third-party sources can be correlated with data ingested in Splunk software to meet the control.

Support
The Splunk platform provides flexible features that help security professionals with controls that are largely policy and process based.

Please also refer to attachment:
SPLUNK AND THE CIS CRITICAL SECURITY CONTROLS.PDF

ii. Identify the security best-practices framework you would recommend for Commission adoption and explain why.

Why is the Splunk's implementation of CIS CSC Important? There are several reasons that organizations embrace the CIS CSC as they develop security strategies:
• Implementation of the controls can reduce the risk of currently-known high priority attacks as well as attacks expected in the near future, as well as provide more high-fidelity data for "hunting"

approaches to protection.
• The controls were generated by consensus from experts in both the federal government and private industry.
• The controls are well written, approachable and distill common security requirements into a list that is easy to understand and implement.
• The controls are reasonably comprehensive and address the most important areas of concern.
• The controls are regularly updated to better reflect the changing threat landscape.

6. Security Framework for Cloud Providers
    i. Identify the key elements and value of standardized security requirements for cloud-based solution providers.

    Splunk believes that cloud based security requires most of the same best practices as on premise but with additional controls. Please refer to C, 2,i above in regard to forwarding data to the cloud for more information on encrypting and transmitting data to the cloud. In addition, Splunk Cloud provides the same capabilities of Splunk Enterprise in a fully hosted and managed environment, which can uniquely be configured in a “hybrid” manner so that data residing both in the cloud and on-premise can be searched from a single platform. Splunk ES is also available within Splunk Cloud.

    ii. Identify and explain the security best-practices framework you would recommend the Commission adopt for cloud services. Explain how this framework differs from security best-practices you would recommend for on-premises systems.

    Splunk maps to the CIS CRITICAL SECURITY CONTROLS as a framework for security Best Practices both on premise and cloud. However, data transmission as an additional control is stated above.

    iii. Identify the key elements and value of standardized due diligence guidelines for utilities when selecting cloud-based solution providers. Explain how this guidance is different from selecting on-premises solutions.
    iv. Identify the cloud services selection guidelines you would recommend for Commission adoption and explain why.
7. Best Practices
    i. Describe how best practices in protecting sensitive utility and

customer information differ between cloud-based hosting and on-premises hosting.

Please refer to C, 2,i above in regard to forwarding data to the cloud.

8. Compliance
    i. Describe whether and how cloud based solutions can improve utility compliance, privacy, and data security.

Hundreds of customers use Splunk Cloud as a single platform to automate compliance for a wide range of government and industry regulations, governance frameworks and internal requirements, including PCI, HIPAA, FISMA, GLBA, NERC, SOX, EU Data Directive, ISO, COBIT and the 20 Critical Security Controls. Splunk enables customers to create correlation rules and reports to identify threats to sensitive data or key employees and to automatically demonstrate compliance or identify areas of non-compliance in regards to technical controls.

The Compliance Challenge
Reporting on firewall, access control and application logs and machine data to demonstrate compliance controls is difficult and costly. Each of these systems generate logs in different formats and locations. Each auditor request involves a different, manual procedure. But the requirement to limit access to production systems has an even bigger impact. System administrators and developers are denied access to production systems to analyze logs and configurations, limiting their ability to respond to operations and security incidents.

Enter Splunk
Bring powerful indexing, search, alerting and reporting to the challenges of change management. With Splunk you can search, alert and report on machine data from virtually any source. Meet compliance requirements from audit trail collection and reporting, to file integrity monitoring with a single solution. Generate any compliance report in seconds. And you'll overcome the operational impact of demands to restrict production system access by giving developers and application support secure, read-only access to the machine data they need without touching production systems.

FISMA
FISMA and NIST standards require federal government agencies have the ability to effectively respond to incidents by analyzing massive amounts of data from large network and IT infrastructures.

Splunk scales to provide visibility into the security technologies in large network infrastructures. Powerful search and reporting of results and flexible ways to organize and tag systems with inventory information and enable the creation of status views for different security controls or locations.

NERC CIP

The North American Electric Reliability Corporation (NERC) has developed mandatory Critical Infrastructure Protection (CIP) Cyber Security Standards to protect the Critical Cyber Assets that control or affect the reliability of North American bulk electric systems. Approved by the Federal Energy Regulatory Commission (FERC), compliance with these standards is mandatory for all organizations involved with the country's bulk electrical network. Splunk Enterprise Security Cloud can be used to monitor, report and track against these standards as a part of an overall Splunk based compliance effort.

SCADA Security

SCADA security compliance requires that proper controls are put in place to minimize risks associated with industrial control systems, which monitor and control processes for delivering critical resources such as electric power, water, oil and gas. Alongside other measures, SCADA system operators must ensure that the control network is kept entirely separate from other network segments to maximize security. Splunk leverages Kepware for industrial level integration, SCADA data forwarding and in turn, SCADA compliance.

The Kepware Industrial Data Forwarder for Splunk plug-in connects Operations Technology (OT) with Information Technology (IT), extending the KEPServerEX communications platform and enabling Big Data and the Internet of Things (IoT). The Industrial Data Forwarder for Splunk takes advantage of the 150+ communications drivers supported by KEPServerEX to seamlessly stream real-time industrial sensor and machine data directly into Splunk software and cloud services, enabling users to search, monitor, analyze, and visualize machine-generated big data from websites, applications, servers, networks, sensors, and mobile devices.

9. What Should Utilities Avoid Putting in the Cloud?
    i. Describe the utility functions - including generation, transmission, distribution, metering, consumption, customer data management and customer experience - that should not be placed in the cloud and explain why. Would your answer depend on whether the information was placed in a public versus private cloud?

Typical Splunk Enterprise Security Cloud sources include the following, other data sources may be avoided by discretion of client:

- Proxy Servers
- Intrusion Detection
- Endpoints, Hosts & related endpoint security providers
- Windows & Linux host events
- Vulnerability Scanner output
- Network packets & Netflow
- Database logs
- Firewall logs
- Threat Intelligence
- Authentication sources such as Active Directory & LDAP
- Wire data over various protocols such HTTP/SNMP/SMTP and others as necessary & supported by Splunk

10. Connectivity
    i. Describe how existing utility IT systems that are not currently interconnected can be made to integrate if hosted in the cloud. What are the benefits and vulnerabilities introduced by interconnecting various utility IT services?

    Splunk Enterprise Security Cloud uses on premise Universal & Heavy forwarder which encrypt and stream data into the Cloud for security analytics. Systems that make up a technical or functional domain can then be aggregated or topologically related once ingested in the Cloud platform by a set of dynamic or pre-configured rules.

Regulatory Barriers:

A. Ratemaking Treatment
    1. Does current ratemaking practice discourage Illinois utilities from deploying cloud-based solutions (e.g., data analytics) provided by third party vendors?
    2. Describe any reasonable justification for accounting ratemaking distinction between investing in cloud-based solutions and investing in on-premises solutions.
    3. Describe whether and how utilities are adopting cloud-based solutions despite its accounting treatment.
    4. Identify alternative ratemaking treatments that would render Illinois utilities indifferent in either choosing to deploy cloud-based solutions provided by third party vendors or continuing with on-premises IT systems owned by the utility.
        i. For each alternative identified, identify the costs and benefits of implementing that alternative.

ii. For each alternative identified, identify Illinois administrative rules that would need to be revised, and the revisions(s) required, in order to implement that alternative.

B. Other Barriers:

1. Identify and explain any other regulatory barriers that discourage Illinois utilities from deploying cloud-based solutions (e.g., data analytics) that would otherwise be in the best interest of the utility and its customers. For each barrier identified, identify Illinois administrative rules that would need to be revised, and the revision(s) required, to eliminate that barrier.

Additional Benefits of Cloud Deployment:,

1. Describe the types of cloud-based technologies available for electric, gas, and water utilities.
2. In electric utilities:
    i. Identify specific software services not currently deployed in Illinois available to engage customers in distributed generation, distributed storage, demand response, and energy efficiency programs. Are those tools available as on-premises and cloud solutions, or is only one option available?
    ii. Identify specific services not currently deployed in Illinois that could provide customer engagement portals that improve customer engagement, increase customer satisfaction, and help meet regulatory mandates for verified energy savings and demand reduction.
3. In water and gas utilities:
    i. Identify the types of software or services not currently deployed in Illinois that could improve customer engagement and increase customer satisfaction.
    ii. Identify the types of software or services not currently deployed in Illinois that could detect leaks and inefficiencies, improve conservation, and lower operating costs.
4. Describe any additional feature benefits to a utility when adopting a cloud-based solution. For example, what are the benefits of cloud software that analyzes consumption patterns, identifies malfunctioning meters, reduces unbilled energy, or engages in predictive maintenance and load forecasting, among other things.

V. Form and Content of Documents Distributed in this NOI

Pursuant to Section 1700.350 of the Commission's NOI rules:

a) An original and three copies of all comments, reply comments, and other documents should be submitted to the Chief Clerk of the Commission on

or before the date stated in the NOI. The distribution of such copies will be as follows:

1) Chief Clerk — Springfield

2) Chicago Office

3) Office of Chairman & Commissioners — Chicago [successor to PAR Division for purposes of this NOI]

b) Copies of all documents filed in the proceeding will be available for public inspection at the Chief Clerk's office in Springfield and the Commission's Chicago office.

c) A copy of the list of participants may be acquired from the NOI Manager. The NOI Manager will take steps to ensure that copies of all documents filed in the proceeding are posted to the Commission's website, www.icc.illinois.gov. In addition to providing comments and other documents as set forth above, interested persons and entities are requested to email the same in electronic form (preferably Adobe pdf) to emcerlean@icc.illinois.gov and apalivos@icc.illinois.gov.

VI. Schedule

The schedule for this NOI shall be as follows, unless altered by the NOI Manager with adequate public notice provided:

- Submission of initial comments (pursuant to 2 Ill. Adm. Code 1700.340 (b)):

  March 31, 2016.

- Submission of reply comments (pursuant to 2 Ill. Adm. Code 1700.340 (c)):

  April 21, 2016.

The Commission anticipates that additional rounds of comments might be of benefit and therefore authorizes the NOI Managers to schedule further rounds, with adequate public notice provided, if they believe that additional comments would be helpful.

Participants are encouraged by the Commission to share their data and other

information pertinent to the issues to be addressed in this NOI with other participants, if requested.

Initiated this 10th day of February, 2016.

(SIGNED) BRIEN SHEAHAN

Chairman